REMARKS

The above-noted cancellation of claims 1-25, and addition of new claims 26-86, as well as the submission of a new Abstract, corrected Specification and substitute Specification, are respectfully submitted prior to initiation of the prosecution of this application in the U.S. Patent and Trademark Office.

The above-noted new claims are respectfully submitted in order to more clearly and appropriately claim the subject matter which applicant considers to constitute his inventive contribution. No new matter is included in these amendments. In addition, the revisions to the Abstract and Specification are submitted in order to clarify and correct the Abstract and Specification and to conform them to all of the requirements of U.S. practice. No new matter is included in these amendments.

In view of the above, it is respectfully requested that these amendments now be entered, and that prosecution on the merits of this application now be initiated. If, however, for any reason the Examiner does not believe such action can be taken, it is respectfully requested that the Examiner telephone applicant's attorney at (908) 654-5000 in order to overcome any objections which the Examiner may have.

If there are any additional charges in connection with this requested amendment, the Examiner is authorized to charge applicant's Deposit Account No. 12-1095 therefor.

Dated: September 26, 2002

Respectfully submitted,

By E. Russ

Lawrence E. Russ
Registration No.: 35,342
LERNER, DAVID, LITTENBERG,
KRUMHOLZ & MENTLIK, LLP
600 South Avenue West
Westfield, New Jersey 07090
(908) 654-5000
Attorneys for Applicant

~~DESCRIPTION~~

INFORMATION TRANSMISSION SYSTEM ~~and~~ AND METHOD, TRANSMITTING APPARATUS, RECEIVING APPARATUS, DATA PROCESSING DEVICE ~~and~~ AND DATA PROCESSING METHOD, AND RECORDING MEDIUM

~~Technical Field~~ BACKGROUND OF THE INVENTION

[0001] ~~This~~The present invention relates to an information transmission system and method, ~~a~~ transmitting apparatus, and receiving apparatus~~, and is suitably applied to an~~ for delivering information over a transmission ~~system which is to transmit information~~ path, such as via a satellite~~, for example~~. In addition, ~~this~~ the invention relates to a data processing device, a data processing method, and a recording medium, and in particular, relates to data processing devices, data processing methods and recording media ~~which are capable of easily restricting terminals (user) to obtain data when the data is broadcasted through a satellite circuit for example.~~ for easily restricting user terminals from obtaining broadcast data, such as data broadcast over a satellite circuit.

~~Background Art~~

[0002] ~~The conventional~~Conventional digital satellite broadcasting ~~system utilizes a~~ systems utilize conditional access (CA) in which ~~the~~ only ~~those~~ legitimate subscribers who have signed up ~~a contract~~ or contracted for reception are allowed to receive the broadcast.

[0003] In ~~such a~~ conditional access, a private key is given in advance to ~~those~~ subscribers who have signed a contract for reception. ~~The~~ A transmitter encrypts the broadcast data, using the private key, ~~to transmit~~ and transmits the data via a satellite. Then, the subscribers decode the received encrypted ~~waves~~ signals using the private key, which ~~allows the~~ permits only those subscribers ~~having made a contract~~ who have contracted for reception to watch and listen to the broadcast.

[0004] In recent years ~~a~~, satellite data transmission ~~system is considered, which is to perform transmission of data in~~ systems may transmit as part of a digital satellite broadcasting system. ~~Since~~ Because the satellite circuit ~~is rapid in transmission speed compared to such circuits as the telephone circuit and ISDN, it has a merit of transmitting a large amount of data in a short time.~~ has a much faster transmission speed when compared to other systems, such as standard telephone circuits and ISDN, large amounts of data may be transmitted in a short time.

[0005] In ~~this~~the satellite data transmission system, ~~if~~ various reception controls ~~can~~ may be used ~~in~~ for (i) general message communication to transmit the same data to all ~~the recipients (this is called “broadcast” hereinafter), and~~ recipients (known as a “broadcast”), (ii) group communication to transmit the same data to a ~~certain~~ specific group of recipients ~~(this is called multicast hereinafter), in addition to an~~(known as a multicast), or (iii) individual communication to transmit a different set of data to ~~individuals (this is called “uni-cast” hereinafter), the usability of the~~ each individual (known as a “uni-cast”). Thus, the potential uses for a satellite data transmission system ~~may increase~~ are significantly increased.

[0006] The~~However, the~~ conditional access system, however, has ~~a~~ the problem that reception control ~~can not~~ cannot be ~~utilized in the~~ used for a uni-cast ~~and~~ or multicast communication because ~~it~~ this system is designed ~~on~~ with the assumption that all the recipients ~~always~~ receive and watch the same information.

[0007] Further, ~~It is possible to secure~~ a greater plurality of channels may be delivered in the same band as ~~the case of transmitting data~~ digital data that is transmitted in the form of analog signals~~, and to provide~~. Also, higher quality ~~of~~ images and sounds~~, when transmitting images, and sounds, etc.~~ are provided when transmitted in the form of digital data~~, so that in such a field as~~. Thus, satellite broadcasting and satellite communication~~,~~ systems ~~are increasingly diffusing~~, which ~~is to~~ provide images and sounds in the form of digital data, are proliferating. Such digital satellite broadcast services ~~are commenced as~~ include SkyPerfect TV! and DirecTV in Japan, DirecTV in ~~US~~ the United States, and Canal Plus in Europe~~, for example~~. The digitalization of broadcasts ~~makes it possible to reduce~~ reduces the broadcast ~~costs~~ cost per channel~~,~~ and ~~to provide~~ provides programs and data that are processed by ~~the~~ computer. Also, ~~because of such~~ digitalization~~,~~ permits the widespread use of services ~~are spreading,~~ in which programs, images, etc. are provided ~~linking~~ that are linked to each other.

[0008] In a digital satellite broadcast ~~services the~~ service, digital data ~~of~~ representing images and sounds ~~is~~ are converted into a format ~~based on~~, such as the ~~MPEG (~~Moving Picture Experts Group ~~) 2, or DVB (~~(MPEG)2 format or the Digital Video Broadcasting ~~)~~(DVB) format which is derived from the MPEG 2, and ~~furthermore,~~ then multiplexed ~~to be transmitted~~ for transmission in the form of radio waves. ~~Received by a~~ The radio waves are transmitted and received by the transponder of a satellite, where the radio waves are amplified~~,~~ and subjected to other ~~necessary~~ processes ~~to be transmitted~~ for re-transmission to the earth.

[0009] The transmission band for the transponder ~~is~~ may be as ~~big~~ wide as 30Mbps ~~(Mega bit~~(Megabits per second)~~,~~ so that ~~it is possible to distribute~~ digital data of high quality may be distributed at high speed utilizing the whole ~~of such a big band. (Note, however, that, even though the transponder has a transmission band of 30Mbpsa~~ width of the band. Though the actual transponder transmission band is 30Mbps, a real transmission band ~~would be somewhere~~ is around 27Mbps, at most ~~because~~, to allow the inclusion of error correction codes ~~are generally affixed.)~~.

[00010] ~~However, generally~~Generally, the transmission band for the transponder is ~~used by being~~ divided into many ~~for~~ bands of multiple channels~~, because of costs. In this case, although~~ to reduce cost. Though the content of the digital data transmitted on each channel ~~is different, a~~ differs, the mechanism ~~of~~ by which the receivers ~~which~~ receive the digital data on each channel remains the same ~~or common~~. Consequently, a conditional access (CA) mechanism is ~~necessary for allowing~~

~~the only limited users to receive digital data provided.~~ needed to allow only permitted users to receive the digital data.

[00011] ~~That is to say, in the case of performing so-called data broadcasting in particular, as~~For data broadcast, in particular, the quantity of data per program is ~~smaller~~ small when compared to the ~~case of distributing~~ images or sounds~~,~~ distributed so that a charging unit or charging system is expected to become more complex. Therefore, a conditional access mechanism capable of performing more specific reception control is needed to ~~cope with~~ address such a problem. The conditional access mechanism is also required to prevent ~~leakage~~ passage of secret information ~~in~~ during distribution.

[00012] Generally, ~~the~~ conditional access ~~mechanism is realized~~ is attained by performing encryption on a data stream ~~to be~~ before it is distributed. ~~As to~~ Two types of encryption methods~~, two types~~ are known, ~~roughly;~~ namely (i) a common key cryptosystem~~(~~, also known as a private key cryptosystem~~),~~, and (ii) a public key cryptosystem. ~~In~~ For digital satellite broadcasting, the common key cryptosystem is more ~~often used~~ common because of a ~~lighter load~~ smaller number of encryption/decryption processes are used when compared to the public key cryptosystem.

[00013] In the common key cryptosystem, a row of codes ~~being~~ that comprise a decryption key ~~equivalent~~ and correspond to an encryption key is given to a ~~certain~~ subscriber A by some method~~, and data~~. Data is encrypted ~~with~~ for distribution using the encryption key ~~for distribution~~. The encrypted data

is designed ~~so as~~ to make it hard to ~~analogize~~ derive the encryption key~~(decryption key) and~~, decryption key or the original data ~~by means of~~, whether by converse calculations or other means. ~~Accordingly, an un~~ Thus, a non-subscribed user B ~~can not~~ cannot accurately restore the original data ~~correctly~~ even if ~~receiving~~ the user B receives the encrypted data. On the other hand, the subscribed user A can restore the original data by decrypting the encrypted data ~~with the use of~~ using the decryption key given when the contract is made. Therefore, the making of a contract for reception ~~subscription~~ is equivalent to reception of ~~the~~ a decryption key.

[00014] ~~By the way, in the case that both~~ When both users A and C are subscribers, for example, ~~when~~ and the contract with A expires, or when the user A does a wrong ~~things~~ action, the current encryption key is changed, and a decryption key equivalent to the new encryption key is provided to user C only. ~~Thereby~~ Thus, the user A who was previously a subscriber or did ~~the~~ a wrong ~~things can not~~ act cannot decode data ~~which is~~ encrypted with the new encryption key, ~~while~~ whereas the legally subscribed user C can ~~normally~~ readily decode the data~~, which is~~ encrypted with the new encryption key~~, with the new decryption key, without problems~~.

[00015] It is ~~troublesome~~difficult, however, to alter an encryption key, and ~~furthermore~~ it is further difficult to provide a new decryption key ~~equivalent~~ corresponding to ~~the~~ a new encryption key to ~~a~~ lawful ~~subscriber every time when~~ subscribers whenever the subscription of ~~a~~ another user expires or ~~when~~ whenever improper ~~conducts are~~ conduct is discovered.

~~Description of the Invention~~

SUMMARY OF THE INVENTION

[0016]The present invention ~~is made in consideration of the foregoing points, and intended to propose~~ provides an information transmission system and method, ~~and~~ transmitting apparatus, and receiving apparatus that are capable of performing reception control in various modes. In addition, the present invention ~~is intended to be able to~~ easily ~~restrict~~ restricts users ~~to~~ that can obtain ~~(~~(or receive) data correctly.

[0017]~~In order to~~To solve such problems, ~~in~~ an information transmission method according to an aspect of the present invention ~~of transmitting~~ transmits data from a transmitting apparatus through a predetermined transmission circuit to a plurality of receiving ~~apparatuses~~ apparatus, each having an individual address~~, when~~. When the data is individually transmitted to the receiving apparatuses, an individual address ~~of~~ for each receiving apparatus is affixed to the data~~, and when~~. When common data is transmitted to a certain group of receiving ~~apparatuses~~ apparatus, the data is affixed with common address information denoting ~~the common~~ a portion of their addresses that is common to all the receiving apparatuses of the voluntary group, ~~and~~ as well as with address range information defining the portion that is common to all the addresses. ~~Then, the~~ The data is received~~,~~ and ~~can be~~ is decoded only when the individual address and the address affixed to the data coincide ~~with each other, and~~ or only when the individual address and the common address information affixed to the data agree with each other within the portion denoted by the address range information.

[0018]According to another aspect of the invention, an information transmission method transmits data from a transmitting apparatus through a specified transmission circuit to a plurality of receiving apparatuses, each having an individual address. When common data is transmitted to the receiving ~~apparatuses~~ apparatus of a certain group, the data is affixed with common address information denoting ~~the common~~ a portion of their addresses common to the receiving apparatuses of the voluntary group, ~~and~~ as well as address range information defining the common portion of the address. On the side of receiving apparatuses, the individual address and common address information affixed to the data are compared based on ~~a basis of~~ the range denoted by address range information, and when the results of the comparison coincide with each other, the data can be decoded, thus easily performing reception control in various modes ~~in easy structure~~.

[0019]A data processing device according to a further aspect of the present invention comprises retrieving means for retrieving, as the marked entry, an entry having an address coinciding with the address of a data block ~~from and~~ by referring to a table ~~containing~~ having addresses and entry validity information ~~indicating~~ that indicate whether the entry to which the address is registered is valid~~, judgment mean for judging~~. Judgment means judges whether the marked entry is valid based on the entry validity information registered to the marked entry~~, and output~~. Output control means ~~for controlling~~ controls the output of data arranged in the data block based on the judgment result obtained by the judging means.

[0021]When the marked entry is valid, the output control means outputs the data at an address arranged in the data block~~,~~ and ~~can~~ may destroy the data when the marked entry is not valid.~~,~~ Furthermore, when the data is encrypted, the data processing device may be provided with ~~an~~ a decoding means for decoding the encrypted data.

[0022]~~When the~~The data ~~is~~ may be encrypted ~~with~~ using a key assigned to the address of the data~~, and when each~~. Each entry of the table ~~has~~ may have a registered key assigned to the address, in addition to the data address, and entry validity information~~, the~~. The decoding means ~~can~~ may decrypt the data with the use of the key registered on the table.

[0023]The decoding means ~~can~~ may decode ~~the~~ data arranged in the data block ~~with~~ using the ~~use of the~~ key ~~on~~ within the table assigned to the address of the data block. Key ~~When key~~ validity information indicating whether the key is valid ~~is~~ may be registered to each entry ~~on the table, in addition to the address, entry validity information, and the key, the decoding means judges~~ in the table. The decoding means may judge whether the key is valid based on the key validity information of the key assigned to the address of the data block, and if the key ~~turns out to be~~ is valid, the data ~~can~~ may be decoded with the use of that key.

[0024]More than two keys assigned to ~~that~~ the address ~~can~~ may be registered to each entry of the table, in addition to the address and entry validity information. Key validity information indicating whether one or more of the keys are valid may be registered to ~~To~~ each entry of the table ~~can be registered key validity information indicating whether the key is valid as to each of more than two keys~~.

[0025]~~A~~The data processing device ~~employing~~ of the present invention may be furthermore provided with table storage means for storing the table. The address may be the ~~MAC (~~Media Access Control ~~)~~(MAC) address of a communication terminal ~~to receive~~ that receives data. Data blocks may conform to the Digital Video Broadcasting (DVB) specifications. The ~~specifications of the DVB (Digital Video Broadcasting).A~~ data processing device employing the present invention may be ~~produced of a one-chip IC (Integrated Circuit).~~ a one-chip Integrated Circuit (IC).

[0026]~~A~~According to a still further aspect of the invention, a data processing method ~~employing the present invention is characterized by and comprises the retrieval step of retrieving as the marked entry~~ comprises retrieving, as the marked entry, an entry having an address coinciding with the address of a data block ~~from and~~ by referring to a table ~~containing~~ having addresses and having entry validity information ~~indicating whether an entry to which the address is registered is valid, judgment step of judging whether the marked entry is valid~~ that indicates whether the entry is valid. The validity of the marked entry is judged based on the entry validity information registered to the marked entry~~,~~ ~~and output control step of controlling the~~. The output of data arranged in the data block is controlled based on the judgment result obtained ~~by the judging means~~.

[0027]A recording medium according to yet another aspect of the present invention ~~is characterized by and comprise the retrieval step of retrieving~~ comprises instructions for retrieving, as the marked entry, an entry having an address coinciding with the address of a data block ~~from and~~ by referring to a table ~~containing~~. The table contains an address and contains entry validity information ~~indicating~~ that indicates whether the entry to which the address is registered is valid~~, judgment step of judging whether~~. The validity of the marked entry is ~~valid~~ determined based on the entry validity information registered to the marked entry~~, and output control step of controlling the~~. The output of data arranged in the data block is controlled based on the judgment result obtained by the judging means.

[0028]~~A~~According to an additional aspect of the invention, a data processing device, data processing method, and recording medium retrieve, as the marked entry, an entry having an address coinciding with the address of a data block ~~from~~ and ~~referring~~ refer to a table containing an address ~~and~~ as well as containing entry validity information indicating whether the entry to which the address is registered is valid. ~~And, judgment is made on whether~~ Whether the marked entry is valid is judged based on the entry validity information that is registered to the marked entry~~, based on the result of which~~

~~the~~. The output of data arranged in the data block is controlled based on this result.

[0029]According to the data processing device, the data processing method and the recording medium ~~employing the present invention~~, an entry having an address matching the address of a data block is retrieved as the marked entry from a table~~,~~ by referring to the same table ~~having~~ that has an entry registering an address and entry validity information indicating whether an entry to which the address is registered is valid. ~~And, it~~ It is judged, based on the entry, whether the validity information registered to the marked entry whether the marked entry is valid~~, based~~. Based on ~~the~~ this result ~~of which~~, the output of data arranged in a data block is controlled. ~~As a result~~ Thus, it is possible to easily restrict the users that are capable of obtaining data normally.

~~Brief Description of the Drawings~~

BRIEF DESCRIPTION OF THE DRAWINGS

[0030]Fig. 1 is a block diagram showing the ~~whole~~ structure of a satellite data transmission system according to an embodiment of the present invention.

[0031]Fig. 2 is a block diagram showing the ~~circuit~~ structure of ~~a~~ the receiving ~~apparatus.~~device shown in Fig. 1.

[0032]Fig. 3 is a schematic diagram showing a header format.

[0033]Fig. 4 is a schematic diagram showing ~~relations~~ the relation between ~~masks~~ a mask and the MAC addresses.

[0034]Fig. 5 is a schematic diagram showing the data structure of a key table.

[0035]Fig. 6 is a flowchart ~~explaining~~ illustrating the steps of a decode processing operation of the invention.

[0036]Fig. 7 is a block diagram showing ~~a structural~~ an example of ~~an embodiment~~ the structure of a broadcast system employing the present invention.

[0037]Fig. 8 is a flowchart ~~explaining the processing by a transmission system 101 in Fig. 7.~~illustrating the steps of the processing operation of the invention carried out by transmission system shown in Fig. 7.

[0038]Fig. 9 is a diagram showing the format of a section and a section header.

[0039]Fig. 10 is a block diagram showing ~~a structural example~~ the structure of a receiving apparatus ~~122~~ shown in Fig. 7.

[0040]Fig. 11 is a diagram showing a key table.

[0041]Fig. 12 is a flowchart ~~used in explaining the processing by a~~ illustrating the steps of a processing operation performed by the receiving apparatus ~~122~~ shown in Fig. 10.

[0042]Fig. 13 is a block diagram showing ~~a structural~~ an example of ~~an embodiment of a computer~~ a processor employing the present invention.

~~Best Mode for Carrying Out the Invention~~ DETAILED DESCRIPTION

[0043]~~Hereinafter, an embodiment~~Embodiments of the present invention ~~will be~~ are now explained in detail with reference to the drawings.

(1) First Embodiment

(1-1) Whole Structure of Satellite Data Transmission System

[0044]~~In~~Fig. 1~~, a reference numeral 1~~ shows ~~the whole~~ a satellite data transmission system 1 to which the present invention is applied~~, and which consists of~~. The system 1 includes a transmission system 2, a satellite 3, and a plurality of reception systems 4 each having substantially the same structure. The transmission system 2 and each of the reception systems 4 are connected ~~on~~ via the Internet 5. ~~A contract is made in advance on the~~ An agreement permitting use of the satellite data transmission system 1 is typically made in advance between a service provider ~~managing~~ that manages the transmission system 2 and each ~~recipient having~~ of the recipients that have a reception system 4.

[0045]~~In~~The transmission system 2 includes a control device 10, which controls the transmission system 2, ~~a control device 10 to control the whole transmission system 2,~~ a circuit connection device 11, a data server 12, and a transmission processing device 13 which are connected ~~on~~ to each other over a local network 14.

[0046]The control device 10 receives ~~a~~ data read-out ~~demand which is~~ demands that are transmitted ~~from~~ by an information processing device 22 in the reception system 4. ~~Responding~~ In response to the data read-out demand, the control device 10 reads out data from the data server 12 or ~~a~~ from an external data server (not shown ~~in figure) on~~) received via the Internet~~, which~~ 5. The data is then fed to the transmission processing device 13 by the device 10.

[0047]The transmission processing device 13 stores an encryption key correspondence table which ~~shows MAC (~~holds the Media Access Control ~~)~~(MAC) addresses ~~being~~, namely the identification numbers ~~inherent~~ corresponding to the respective information processing devices 22 ~~in the reception systems 4, and~~ , and which holds the private keys ~~corresponding~~ that correspond to each of the MAC addresses. ~~Based on~~ Using the encryption key correspondence table, the transmission processing device 13 encrypts the read data ~~with the use of~~ using a private key ~~matching~~ that matches the MAC address of ~~the~~ an information processing device 22 ~~which~~ that is ~~a~~ the transmission destination. ~~Further, the~~ The transmission processing device 13 ~~makes “0” the~~ then assigns a value of “1” to the ~~CKI (~~Common Key Indicator~~, to be described later) of the data to be transmitted to all the information processing devices 22 as the broadcast and encrypts it~~ (CKI) of the data. Alternatively, the device 13 encrypts the data using a given common key~~. Furthermore, the~~ and assigns a CKI value of "0". The transmission processing device 13 packets the encrypted data in ~~the format defined to the DVB (Digital Video Broadcasting) data broadcast specifications, which is then transmitted~~ accordance with the Digital Video Broadcasting (DVB) data broadcast specification, and a transmitter 15 then transmits the formatted data as an uplink wave S2 to the satellite 3 ~~via the transmission 15~~.

[0048]~~Upon the receipt of~~After receiving the uplink wave S2, the satellite 3 amplifies ~~it~~ the wave and ~~transfers it as~~ re-transmits the ~~downlink~~ wave ~~S3~~ to the reception system 4 as a downlink wave S3. The ~~systems 4.In the~~ reception system 4~~,~~ ~~the~~ includes a receiving device or apparatus 21, ~~the~~ a line or circuit connection device ~~21~~ 23, and a plurality of information processing devices 22 ~~being~~ which may be, for example, personal computers ~~are connected to each other on a local network 24~~. The receiving apparatus 21, the processing devices 22, and the circuit connection devices 23 are connected to one another using a local area network 24.

[0049]The receiving apparatus 21 decodes ~~the~~ data~~, which is~~ transmitted to the information processing device 22~~,~~ by ~~performing~~ demodulation processing and decode processing ~~on~~ the downlink wave S3 that is received via a receiving antenna 20~~, and~~. The receiving apparatus 21 then supplies ~~it~~ the decoded data to the information processing device 22.

[0050]When a user initiates a data read-out demand ~~is made by a user~~, the information processing device 22, ~~responding to it~~ in response to the demand, transmits the data read-out demand to the transmission system 2 via the circuit connection device 23 ~~on~~ via the Internet 5.

(1-2) Structure of Receiving Apparatus

[0051]~~Next, explanation will be given on the~~The receiving apparatus 21 in the reception system 4 is now described in greater detail with reference to Fig. 2. The ~~In the~~ receiving apparatus 21~~,~~ includes a ~~CPU (~~Central Processing Unit ~~) 30 controlling the whole~~(CPU) 30 which controls the receiving apparatus 21~~,~~ and which is connected, ~~with~~ via a bus 39, to a front end unit 31, a demultiplexer 32, a receiving filter 33, a decoding unit 34, a checker 35, a buffer 36, a key table 37, and an interface unit 38.

[0052]The front end unit 31 demodulates the downlink wave S3 that is received via the receiving antenna ~~39, which is fed~~ and feeds the demodulated wave as a data stream D31 to the demultiplexer 32. The demultiplexer 32 separates ~~the only~~ necessary packets from the data stream D31 based on ~~the PID (Packet ID),~~ their Packet ID's (PID's) and supplies ~~them~~ the packets to the receiving filter 33. The receiving filter 33 checks the payloads of the packets ~~supplied from the demultiplexer 32 to destroy packets~~ and eliminates any packets that are unnecessary for data decode processing.

[0053] In accordance with a decoding process ~~to be~~ described ~~later~~ herein, the decoding unit 34 refers to ~~the~~ a key table ~~28 with~~ 37, using the MAC address of the information processing device 22~~(Fig. 1) as the retrieval key~~, to obtain a decoding key from the key table 28. ~~Then, the~~ The decoding unit 34 then decodes the data stream D31 ~~with the use of~~ using the decoding key ~~obtained,~~ and supplies the resultant ~~as the~~ decoded data D34 to the checker 35.

[0054] The checker 35 ~~examines~~ determines whether or not the ~~decoding processing is conducted correctly with regard to the~~ decoded data D34 was decoded correctly. Then, ~~responding~~ in response to a demand from the CPU 30, the buffer 36 inputs the decoded data D34 to the interface unit 38 ~~through~~ via the bus 39. The interface unit 38 then supplies the decoded data D34 to the information processing device 22 ~~on~~ over the local network 24~~(Fig. 1)~~.

[0055] In this ~~way~~ manner, the receiving apparatus 21 receives the downlink wave S3, extracts ~~the~~ only the data that is to be supplied to the information processing device 22, and supplies ~~it to the information processing device 22~~ the data thereto.

(1-3) Decode Processing of Digital Stream

[0056]~~As shown in~~Referring to Fig. 3, the digital stream D31 ~~is affixed with~~ includes packet ~~header~~ information located at the top of ~~the~~ a payload section as well as ~~a~~ stuffing byte ~~(invalid byte) and CRC (~~that indicates the presence of an invalid byte and a Cyclic Redundancy Code ~~)~~(CRC) that are located at the bottom of the payload~~, and~~ section. The digital stream is encapsulated ~~so as~~ to be processed as a section ~~based on~~ defined according to the DVB data broadcasting ~~specifications (Datagram-section). The MAC address#6 means a byte (8 bits) from Bit 7 to Bit 10, with the~~ specification, known as a Datagram-section. The Datagram Section includes a six byte MAC address, identified as MAC address #1 to MAC address #6, each of which is comprised of a byte (8 bits) having bits from Bit D7 to Bit D0. The highest bit of the MAC address ~~as~~ is at Bit ~~47~~ D7 and the lowest ~~as Bit 0.~~ is at Bit D0.

[0057]~~The~~Referring back to Fig. 2, the decoding unit 34 determines whether to receive a packet~~,~~ based on ~~a basis of~~ the MAC address ~~described~~ stored in each packet of the received data stream D31 ~~received and~~ and based on the key table 37. Here, ~~In such packet discrimination processing~~ the receiving apparatus 21 ~~according to the present invention performs~~ may perform (i) a mask bit process to ~~designate a bit position~~ determine the bit positions that are to be compared ~~in~~ with those of the MAC address~~,~~ of a packet, (ii) a MAC address conversion ~~process to~~ which converts the MAC address of a packet into a value having ~~less~~ fewer bits and ~~to discriminate~~ then discriminates packets using the converted value, ~~and~~ or (iii) a MAC address pass process to let the packets having a specific MAC address pass unconditionally.

[0058] The mask bit process ~~is to perform~~ takes a logical product ~~on~~ between the mask bit and the result of a comparison between the MAC address ~~described in~~ of the section header and the MAC address in the key table 37. ~~When the exclusive or is taken as ^, the logical product as &, the MAC address described in the session header as MR, k-th AC address in the key table as MAC (k), and the weight of the bit as 1, the following equation is calculated~~ Specifically, the following relation represents the process carried out for each bit in the range of $0 \le k \le 47$: $(\sim(MR_1\ \hat{}\ MAC_1(k)))\ \&\ MASK_1(k)$ (1), where ^ represents an exclusive OR operation, & represents a logical product, MR_1 is the MAC address read from the session header and stored in the MR register, $MAC_1(k)$ is the k-th MAC address stored in the key table, and $MASK_1(k)$ is the k-th mask value stored in the key table. When the logical product is "0", the masked portions of the two ~~0147.~~

~~(~(MR1 ^MAC1 (k)))&MASK1 (k) ·······(1)~~

~~Only when All the results are "0", both~~ MAC addresses are identical.

[0059] ~~It means that~~Thus, bits of the MR and the MAC ~~address~~ addresses are compared only ~~when~~ where the mask ~~is~~ has a bit ~~of~~ value "1". ~~The~~ Fig. 4 shows an example of the ~~relations~~ relation between ~~this~~ each mask bit and the comparison operation between the ~~MR and the MAC address.~~ MAC address stored in the MR register and a MAC address stored in the key table.

[0060]~~In the case of~~ Fig. 4 shows an example in which the mask bits are “0” from bit D0 to bit D3~~,~~ and are “1” from bit D4 to bit D47. When ~~the~~ a mask address is checked ~~using the mask bits, the sameness of the MAC address and MR in a section from D4 to D47, in which~~ based on the mask bits, a MAC address in the key table and the MAC address in register MR are compared from bits D4 to D47, namely the bits where the mask bits are all “1”~~, is the condition for the identity of the MAC addresses, while the sameness of~~. By contrast, the MAC address and ~~MR does not matter in a section from~~ the register MR need not be the same in bits D0 to D3 where the mask bits are all “0”. Thus, by checking only ~~a~~ part of the MAC addresses using the mask bits, it is possible to ~~conduct the~~ carry out a multicast ~~(group communication) where~~ or group communication whereby the same packets are distributed to certain information processing devices 22 ~~each~~ having ~~a~~ different MAC ~~address.~~ addresses. Also, ~~with~~ when all the mask bits ~~being~~ are “1”, that is~~,~~ “0xFFFFFFFFFFFF”, all the bits of the MAC address are checked, ~~whereby the~~ so that a uni-cast (individual communication) can be carried out.

[0061]~~In~~When carrying out ~~the~~ a multicast using mask bits, it is ~~premised on an assumption~~ assumed that a common part exists in the MAC address of each information processing device 22~~.~~ ~~However it is hard to prepare such information processing devices 22, and besides it is feared that~~ that is to receive the multicast data. However, such MAC addresses are hard to prepare, and further flexibility may be wanted ~~in~~ when running a system. In this case, the problem can be solved by artificially creating a common part in the MAC addresses ~~falsely~~ of the devices 22 by rewriting the packet header ~~on the basis of the~~ based on a correspondence table of the MAC addresses of actual information processing devices 22 and the MAC addresses described in the packet headers.

[0062]The MAC address conversion process ~~is to operate a certain formula (Hash function) with regard to~~ uses a formula, such as a Hash function, for operating on an input MAC address to obtain a value ~~reduced to a bit number smaller than 48 bits, and perform a search on a table (Hash table) describing whether to let it pass,~~ having a smaller number of bits than the 48 bit MAC address and then searches a table, such as a Hash table, to determine whether to let the address pass with the obtained value used as a key. The ~~reason why the bit~~ number of bits is reduced ~~is because~~ so that the Hash table is made smaller. Any Hash function may be used as long as it ~~be~~ is able to distribute input MAC addresses well. For example, ~~obtain~~ for a CRC~~, and assume that the~~ whose higher 6 bits are defined as p, ~~and~~ when Pass (p) ~~is~~= “1”, ~~allow it~~ the packet is allowed to pass, and when Pass (p) = “0”, ~~destroy it~~ the packet is destroyed. Here, the pass function is ~~the~~ a table of $2^6 = 64$ bits. In this way, the circuit scale of the decoder unit 34 can be made smaller by reducing the ~~bit~~ number of bits of a MAC address using the Hash function.

[0063]The MAC address passage process ~~is to let it~~ lets the packet pass if a MAC address described in the header of a packet is an address for a specific broadcast regardless of ~~the~~ its state ~~of~~ in the key table. If ~~an~~ a MAC address described in the header of a packet is of value 0xFFFFFFFFFFFF~~(this address is called~~, known as a “broadcast address”~~), it~~, the message is always ~~reckoned as~~ considered a broadcast and allowed to pass. ~~In the present invention this~~ The MAC address passage process ~~is made~~ occurs prior to the mask bit process and MAC address conversion process. ~~Because of this~~ Thus, it is not necessary to search the key table when the MAC address described in the packet header is a broadcast address, resulting in ~~the improvement of~~ improved process speed.

[0064]In this manner, the decoding unit 34 discriminates packets based on ~~the basis of~~ a MAC address described in the header of a packet, the MAC address of an information processing device 21, and mask bits.

[0065]Subsequently, the decoding unit 34 detects whether or not the above discriminated packets ~~have been~~ are encrypted. If the packets have been encrypted, ~~a~~ decoding ~~process~~ is performed ~~with~~ using a decoding key taken ~~out of the~~ from a key table. For ~~the~~ a broadcast, however, ~~it is necessary to prepare~~ a common key is prepared which is a decoding key ~~shared by~~ that is common to a plurality of MAC addresses.

[0066]The receiving apparatus 21 ~~employing the present invention~~ judges whether to use a common key~~,~~ using the section that is the 6th byte from the highest~~(~~, namely bit D7 of the second byte on the second line in Fig. 3~~). This is called “CKI” (Common Key Indicator) in the present invention.~~

~~It is stipulated that, when the CKI~~. This value is called a Common Key Indicator (CKI). When the CKI value is "1", an individual key is used~~, which~~ and is extracted from the key table ~~by means of~~ using the register MR, the MAC address, and the mask bit~~, and that, when~~. When the CKI value is "0", the common key is used regardless of the setting of the key table. In the DVB data broadcast specifications, the CKI is defined as a "reserved" bit with "1" ~~taken~~ as ~~the~~ its value. A common key ~~being~~ is considered ~~to be rather~~ a special processing method when compared to an individual key, ~~the agreement with the DVB data broadcast specifications is attained by the stipulation~~ so that stipulating that a common key be used when the CKI is "0" attains agreement with the DVB data broadcast specifications.

[0067]Although a special storage area may be prepared for a soaring common key, it is ~~desirable to share~~ preferable to store the data on a special line ~~on~~ in the key table, ~~making~~ so that the read-out process ~~common to~~ is the same as for an individual key ~~as well as enabling the effective use of~~ and more efficiently uses the storage area. Preferably, the starting line, namely the first line ~~should be~~, of the key table is designated as the special line. Because the first line ~~does exist~~ exists regardless of the number of lines n of the key table ~~so that~~, it is possible to retain or retrieve the common key without changing the order of the procedure regardless of ~~the existence of~~ whether receiving apparatuses ~~with~~ exist that have different values of n.

[0068]~~The~~ Fig. 5 shows the structure of the key table 37. The

"MAC address #1" denotes ~~the~~ a 48-bit MAC address described on the first line of the key table, the "mask #1" denotes ~~a mask bit a mask bit corresponding~~ the 48 mask bits that correspond to the MAC address #1, and k_{1Even}, ~~k1Odd denote key data of Even/Odd corresponding to each MAC address #1, having~~ k_{pOdd} denote even and odd key data of that correspond to the MAC address #1. Each of the even and odd key data has a bit width m based on an encryption form. The key table ~~possesses a plurality (n pcs.) of structures similar to the above. The greatest number or upper limit is determined by the circuit scale the key table 28 can have.~~comprises a plurality of n such data structures. The circuit scale of the key table 37 determines the upper limit of the value of n.

[0069]The MAC addresses and the key data each ~~has an~~ have its own independent valid flag~~, making it possible~~ to manage whether the individual values are valid ~~or not individually~~, so that ~~the~~ individual valid flags can be utilized to discriminate MAC addresses as well as key data. Also, because the key table has an independent flag for each line, the key table may contain vacant lines ~~(invalid lines).~~ or invalid lines. Accordingly, ~~what is needed~~ to temporarily nullify the information of particular lines ~~temporarily is to simply make~~, the Valid bits of the MAC addresses are set to "0", which is preferable for a process carried out at high speed. The decoding unit 34 decodes packets ~~with~~ using the ~~use of~~ decoding keys thus obtained.

(1-4) Decode Processing Procedure

[0070]Next, an explanation of the ~~decode processing procedure~~

decoding process for digital streams ~~will be~~ is given with reference to the flowchart ~~in~~ of Fig. 6. The decoding unit 34 starts the processing, shown at step RT1, and ~~after reading~~ writes the 48 bit MAC address of ~~48 bits described in~~ the packet header into a register MR, as shown at ~~the~~ step SP1, and proceeds to the next step SP2.

[0071]At the step SP2, the decoding unit 34 judges whether the value of the register MR is equal to the broadcast address ~~(0xFFFFFFFFFFFF)~~ value, namely the value 0xFFFFFFFFFFFF. When an affirmative result is obtained ~~at~~, the ~~step SP2, it~~ unit 34 denotes that the value of the register MR is equal to the broadcast address, that is ~~to say, this~~ the packet is a broadcast packet. ~~Skipping the~~ Omitting steps SP3 and SP4, the decoding unit 34 moves ~~on~~ directly to the step SP5.

[0072]~~On the other hand~~Alternatively, when a negative result ~~be~~ is obtained at the step SP2 ~~it means~~, namely that the value of the register MR is not equal to the broadcast address~~, that is, this~~ value, the packet is not a broadcast packet. The decoding unit 34 then proceeds to the step shown at SP3.

[0073]~~At the~~As step SP3 shows, the decoding unit 34 searches each line ~~on~~ of the key table ~~from #1 line in order on the basis of the~~ 37, starting from line #1, using the above expression (1) to ~~check to see when~~ determine whether the Valid bits are ~~“1” (namely,~~ of value “1”, namely whether the line is in a valid state~~),~~, and whether ~~there exists~~ valid lines exist where the register MR and the MAC address are equal ~~in~~ for all the bits ~~in~~ of a section having the mask bit of value “1”.

[0074]When an affirmative result is obtained at the step SP3, ~~it means that there exists lines~~ lines exist where the register MR and MAC address are equal in all the bits ~~in~~ of a valid section having the mask bits of value “1”, ~~then~~ and the decoding unit 34 ~~goes on~~ proceeds to ~~the~~ step SP5. Alternatively, when ~~Whereas,~~ a negative result~~, when~~ is obtained ~~at the step SP3, indicates that~~, there is no line where the register MR and the MAC address ~~is~~ are equal ~~in~~ for all the bits ~~in~~ of a valid section ~~having~~ that have the mask bits of value “1”. Then, the decoding unit 34 proceeds to the step SP4.

[0075]~~At the~~As shown at step SP4, the decoding unit 34 creates a Hash value out of the MAC address ~~described in~~ of the packet header ~~with the use of~~ using a Hash function~~, with which~~ and uses the Hash value to retrieve a specific Hash table ~~is retrieved, and it is judged whether a bit corresponding to the Hash value is “1”.~~ value bit. The decoding unit then judges whether the Hash value bit has a value of “1”.

[0076]~~A negative result at the step SP4, when obtained, indicates that~~When a negative result is obtained, the bit of the Hash table ~~is~~ has value “0”~~, and~~ which indicates that ~~this~~ the packet is not a packet that a receiving apparatus 21 is to receive~~, then~~. Then, the decoding unit 34 proceeds to ~~the~~ step SP13 and ~~destroys that~~ eliminates the packet~~, terminating the~~ and terminates processing, as shown at ~~the~~ step SP14.

[0077]On the other hand, when an affirmative result is obtained ~~at the step SP4, it means that~~, the bit of the Hash table ~~is~~ has a value of “1”, and ~~this~~ thus the packet is ~~a~~

~~packet~~ one that the receiving apparatus is to receive. The decoding unit 34 ~~moves on~~ then proceeds to ~~the~~ step shown at SP5.

[0078]~~At the~~As step SP5 shows, the decoding unit 34 ~~judges on the basis of the values~~ determines, based on the value of lower bits of the ~~PSC (~~Payload Scrambling Control ~~) (Fig. 3)~~(PSC) of the packet header shown in Fig. 3, whether the packet ~~has been~~ is encrypted. When a negative result is obtained at the step SP5, ~~it means that~~ the lower bits of value are "0", that is~~,~~ the packet ~~has~~ is not ~~been~~ encrypted. ~~Then, the~~ The decoding unit 34 then proceeds to the step shown at SP14 ~~and~~, transfers the packet to the checker 35 ~~at a later stage~~ without ~~performing an~~ any encryption cancel processing, ~~terminating the~~ and terminates processing.

[0079]~~Whereas,~~ When an affirmative result ~~at the step SP5, when~~ is obtained, ~~indicates that~~ the lower bits are of value "1", namely the packet ~~has been~~ is encrypted. The decoding unit 34 then moves on to the shown at step SP6.

[0080]~~At the~~As shown at step SP6, the decoding unit 34 ~~judges on the basis of~~ determines, based on the value of the CKI ~~(Fig. 3)~~ in the packet header shown in Fig. 3, whether the packet ~~has been~~ is encrypted ~~with the use of~~ using a common key. When an affirmative result is obtained ~~at the step SP6, it means that~~, the CKI is of value "0", ~~that is,~~ namely the packet has been encrypted ~~with the use of~~ using a common key. Then, the decoding unit 34 proceeds to the step shown at SP7~~,~~ and substitutes a value of "1", denoting a common key for the register k, while retaining the retrieval numbers of the keys,

~~moving on~~ and then proceeds to the step shown at SP10. On the other hand, when a negative result is obtained ~~at the step SP6, it means that~~, the CKI is of value "1", that is~~,~~ the packet has been encrypted ~~with the use of~~ using an individual key, ~~then~~ and the decoding unit 34 proceeds to the steps shown at SP8.

[0081]~~At the~~As step SP8 shows, the decoding unit 34 searches the key table, ~~a line after another, based on~~ line by line, using the expression (1), and determines whether ~~there exists~~ a MAC address ~~coinciding~~ exists that coincides with the register MR ~~on~~ of the key table. ~~It should be noted that packets~~ Packets, which should not be received as a result of the discrimination ~~by means of~~ operation using the Hash table ~~at~~ of the step, SP4~~,~~ are allowed to pass ~~should~~ when the Hash values ~~happen to~~ coincide. However, because ~~those~~ these packets are re-discriminated at the step SP8, no decoding processing is carried out ~~on them erroneously~~. Also, ~~note that since~~ because the packets that are not encrypted will not pass through the step SP8, they are ~~destroyed at~~ eliminated by a subsequent circuit or by the information processing device 22.

[0082]The ~~searching of the~~ key table is ~~performed~~ searched from the first line ~~of the key table and on, and checking is repeated~~ until a first coincidence is encountered. ~~Here, a~~ A valid address ~~means~~ indicates that the Valid bits shown in Fig. 5 are in an activated state. As an example, assuming that an active state is ~~referred to~~ the state where the Valid bits are of value "1", ~~it is reckoned that~~ information on the lines with Valid bits of value "0" is invalid. ~~For example~~ Thus, when the Valid bits of the MAC address#2 are "0", ~~those~~ the values are not referred to no matter what value is ~~set~~ assigned to K_{2Even}, K_{2Odd}.

[0083]When a negative result is obtained at the step SP8, ~~it indicates that~~ there are no MAC addresses coinciding with the MR ~~on~~ of the key table, and ~~that this~~ the packet is not ~~a packet~~ one that the receiving apparatus 21 is to receive. ~~Then, the~~ The decoding unit 34 then proceeds to the step shown at SP13, and destroys the packet, thereby terminating ~~the~~ processing, as shown at ~~the~~ step SP14.

[0084]On the other hand, when an affirmative result is obtained ~~at the step SP8, it indicates that there exist~~, MAC addresses exist that coincide with the MR~~, and~~ which indicates that ~~these~~ the packet are ~~packets~~ ones that the receiving apparatus 21 is to receive. The decoding unit 34 ~~moves on~~ proceeds to the step shown at SP9~~,~~ and substitutes, for the register k, the retrieval numbers of the keys with which the MAC addresses coincide under the condition of expression (1), and ~~then~~ the unit 34 proceeds to the step SP10.

[0085]~~At~~As shown at the step SP10, the decoding unit 34 judges, based on the higher bits of the PSC, whether ~~this~~ the packet ~~has been~~ is encrypted with either a key in an Even period or with a key in an Odd period. ~~It is to be stipulated, for example, that when~~ When the higher bits of the PSC are of value "0", the packet is encoded with a key in an Even period, and ~~"1" in an Odd period.~~when the higher bits of the PSC are of value "1", the packet is encoded with a key in an Odd period.

[0086]When the higher bits of the PSC are “0”, the decoding unit 34 retrieves ~~from the key table~~ a key in an Even period from the key table and allocates the values of Valid bits of K_{iEven} ~~oriented~~ to the MAC address #I ~~coincided~~. When the higher bits of the PSC are “1”, the decoding unit 34 retrieves ~~from the key table~~ a key in an Odd period from the key table and allocates the values of Valid bits of K_{iOdd} ~~oriented~~ to the MAC address #I ~~coincided, and then~~. Then, the unit 34 proceeds to the step shown at SP11.

[0087]~~At the~~As step SP11 shows, the decoding unit 34 judges whether the value of the Valid bits retrieved are “1”~~(namely~~, namely whether the function Valid (k, EO)=1~~)~~. When a negative result is obtained at the step SP11, ~~it denotes that~~ Valid (k, EO) ~~is~~ equals “0”, that is~~, even~~ though the packet ~~has been~~ is encrypted, ~~there exists~~ no valid decoding key (individual key) exists. The decoding unit 34 then proceeds to the step shown at SP13~~,~~ and destroys the packet, terminating the processing at the step SP14.

[0088]~~Whereas,~~ When an affirmative result ~~at the step SP11, when obtained, indicates that~~ is attained, namely Valid (k, EO) ~~is~~ equals “1”, that is~~, there exists~~ a valid decoding key (individual key)~~, and then~~ exists, the decoding unit 34 proceeds to the step shown at SP12. As ~~At the~~ step SP12 shows, the decoding unit 34 retrieves a key (k, EO) from the key table 37 ~~a key (k, EO)~~, namely a decoding key ~~corresponding~~ that corresponds to the k^{th} EO, with which the packets are decoded and ~~output to the check~~ later outputted to be checked at a later stage, thereby terminating the processing at the step SP14.

[0089]Thus, the decoding unit 34 performs packet decoding processing ~~suitable~~ for each ~~distribution mode~~ of the unicast, multicast, and broadcast ~~on the basis~~ modes based on of the key table 37 and the Hash table. Because the ~~retrieval processes (steps SP5 to SP13) in the foregoing decoding processing of decoding keys are performed independently~~ key retrieval processes, shown at steps SP5 to SP13, are performed independent of the discrimination processes ~~(steps SP1 to SP4)~~ of the MAC addresses, shown at steps SP1 to SP4, encryption processes ~~can~~ may also be performed on the broadcast addresses~~, too~~. In this case, two common key setup methods ~~can be considered; 1st method~~ are possible: (1) where a common key is designated as ~~a~~ the decoding key with which ~~to communicate with~~ corresponds to the broadcast address, and ~~2nd method~~(2) where the broadcast address is ~~registered on~~ stored in the key table as ~~the~~ a MAC address ~~oriented~~ and corresponds to an individual ~~key.~~ private key.

[0090]~~The 1st~~Using method (1), the system does not consume the storage area of the key table 37, but the system must share a common key with other ~~broadcasts. The 2nd method does consume~~ modes. Using the method (2), the system consumes the storage area of the key table 37~~,~~ but ~~is able to set~~ sets up a decoding key dedicated to ~~the~~ a broadcast.

(1-5) Operation and Effect in this Embodiment

[0091]~~Structured as described hitherto~~Thus, the decoding unit 34 also discriminates packets having the broadcast address

~~("0xFFFFFFFFFFFF)~~ value, namely "0xFFFFFFFFFFFF, based on the MAC address ~~described~~ stored in each packet of the received data stream D31 ~~received~~, and ~~also~~ the unit discriminates the ~~packets of the~~ multicast ~~and uni-cast~~ packets by checking the MAC addresses using mask bits. ~~At this time the~~ The decoding unit 34 also calculates the Hash values of the MAC addresses, ~~based on which the packets of the multicast and uni-cast~~ which determines the uni-cast packets that are discriminated.

[0092]Then, the decoding unit 34 detects whether the discriminated packets ~~have been~~ are encrypted, and when they ~~have been~~ are encrypted, decode processing is ~~perform with~~ performed using a decoding key taken ~~out of~~ from the key table. At this time, the decoding unit 34 judges, based on the CKI of a packet ~~by~~, which key~~,~~ is to be used, namely whether the packet ~~was~~ is encrypted using a common key or a private key, and the packet is decoded with either the common key or private key ~~according to the result.~~ accordingly.

[0093]~~According to the structure described hitherto, a~~A specific MAC address value is ~~used~~ defined as the broadcast address, and only ~~a~~ part of the bits of the MAC address is checked using the mask bits so that various reception controls are available ~~for~~ such as for broadcast, multicast, and uni-cast. Also, the ~~bit~~ number of ~~a~~ MAC address bits is reduced ~~with the use of~~ using a Hash function, and packets are discriminated ~~with~~ using the reduced MAC address, so that the circuit scale of the decoding unit 34 can be reduced.

(1-6) Other Modes of Embodiment

[0094]In the foregoing embodiment ~~a bit of which mask bit is~~

~~located at “1” is subjected to the target of comparison of~~, a bit whose corresponding mask bit is “1” is compared with MAC addresses. However, the present invention is not limited to ~~it~~ using such bits, but to the contrary, a bit ~~of which~~ whose corresponding mask bit is ~~at~~“0” may ~~be the target of comparison.~~instead be compared.

[0095]Also, in the foregoing embodiment, a packet is destroyed when the ~~retrieval~~ result ~~on~~ retrieved from the Hash table ~~turns out~~ is “0”. However, the present invention is not limited ~~to it~~ thereto, but to the contrary, the Hash table may be set up so that a packet is destroyed when the ~~retrieval~~ result ~~of~~ retrieved from the Hash table ~~turns out~~ is “1”.

[0096]Furthermore, in the foregoing embodiment, the MAC address #6 is designated as the broadcast address, but the present invention is not limited ~~to it, but~~ thereto. Thus, another MAC address ~~“0xFFFFFFFFFFFF”~~ having a value other than ~~this~~“0xFFFFFFFFFFFF” may be designated as the broadcast address.

[0097]Furthermore, in the foregoing embodiment, processing is performed in the order of ~~the discrimination of~~ first discriminating broadcast addresses in the decode process (Step SP2), then checking ~~of~~ MAC addresses on the key table (Step SP3), and ~~retrieval of~~ thereafter retrieving the Hash table (Step SP4). However, the present invention is not thus limited ~~to it,~~, and decode processing may be carried out in another order.

[0100]Furthermore, ~~in~~ the foregoing embodiment ~~explanation is given on the case~~ is explained where the present invention is applied to a satellite data transmission system. However, the present invention is not thus limited ~~to it, but~~ and may be applied to other data transmission systems such as a cabled Internet, for example.

(2) Second Embodiment

[0101]~~The~~Fig. 7 shows a structural example of ~~one~~ another embodiment of a broadcasting system ~~employing~~ of the ~~present~~ invention. ~~(Note that~~ Here, the system ~~here means that~~ comprises a plurality of devices that are logically assembled~~,~~ ~~and it does not matter~~ regardless of whether ~~each device is~~ the devices are housed in the same ~~housing.)~~housing.

[0102]In the embodiment shown in Fig. 7 ~~a broadcasting~~, a broadcast system ~~consists of~~ includes a transmission system 101, a satellite 102, a reception system 103, and a network 104. To avoid ~~the~~ unneeded complexity ~~of the figure the~~, only one reception system ~~(reception system 103) for the 101~~ 103 is shown in Fig. 7~~, however,~~ though two or more ~~than two~~ reception systems may be employed.

[0103]The transmission system 101 comprises a control device 111, a data server 112, a transmission processing device 113, an antenna 114, a circuit connection device 115, and a cable 116~~, and the~~. The control device 111, the data server 112, the transmission processing device 113, and the circuit connection device 115 are connected to each other ~~with~~ via the cable 116~~, which constitutes a LAN (~~ as part of a Local Area Network (LAN).

[0104]The control device 111 ~~lets~~ enables the transmission processing device 113 to supply data ~~to be distributed in~~ for distribution by satellite ~~broadcasting~~ transmission by its controlling the data server 112. Also, the control device 111 controls and ~~lets~~ permits the circuit connection device 115 to obtain data ~~to be distributed in satellite broadcasting~~ from an external network 104, such as via the Internet, and lets the transmission processing device 113 provide ~~it~~ the data. Furthermore, the control device 111 controls various processes in the transmission processing device 113.

[0105]The data server 112 retains data that is to be distributed ~~in~~ by satellite ~~broadcasting,~~ transmission and supplies necessary data to the transmission processing device 113 under the control of the control device 111. The transmission processing device 113 packets the data that is supplied from the data server 112 and from the circuit connection device 115 into ~~IP (Internet Protocol)~~ Internet Protocol (IP) packets under the control of the control device 111, and ~~furthermore~~ the device 113 blocks the IP packets into data blocks ~~called a section described by the describer based on the multiprotocol Encapsulation regulated in e.g. ~~, known as sections, according to the multi-protocol encapsulation standard defined in, e.g., EN 301 192 V1.1.1 (1997-12), the DVB specification for ~~data broadcasting ETSI (~~European Telecommunications Standards Institute ~~). And, the~~(ETSI) for data broadcasting. The transmission processing device 113 divides a section into payloads each having a given length, and each payload is appended with the header of a packet ~~forming a transport stream (referred to as a TS (Transport Stream)), resulting in the formation of a packet of a kind of~~

~~TS packet, to which further processes such as~~ to form a transport stream (TS) which is further processed, such as using modulation and amplification ~~are applied,~~, and which is finally transmitted as satellite broadcast waves via the antenna.

[0106]Also, the transmission processing device 113 has the MAC address of each of terminals 124_1, 124_2, ···~~(as~~, shown in Fig. 7, as well as of terminals ~~forming a reception system~~ not shown in Fig. 7~~) forming~~, to form a reception system 103~~, and~~. The device 113 includes an encryption key table storage unit 113A for storing an encryption key table in the form of a diagram oriented to the encryption key assigned to each MAC address~~(Media Access Control). Note that all~~. All the encryption keys assigned to each of the MAC addresses are basically different. However, the same encryption keys may be assigned to some of the MAC addresses.

[0107]~~Just for additional information, the~~The MAC address is a system of ~~an address applicable~~ addresses according to the ~~IEEE (~~Institute of Electrical Electronics Engineers ~~)~~(IEEE) 802.3 standard, etc., and is an individual value of 48 bits for each communication port. The 48-bit MAC address ~~of 48 bits consists of the~~ includes a higher ~~half~~ 24 bits ~~being~~ which are an identification number of a manufacturer ~~(~~(or vendor) registered to and supervised by the IEEE~~, and the~~. The lower ~~half~~ 24 bits ~~being~~ are a device identification number supervised by each vendor. Using the MAC address, an address of each of the terminals 124_1, 124_2,··· can be specified.

[0108]According to the foregoing multiprotocol encapsulation, ~~in the header of a section (section header) is arranged~~ located within the section header is the MAC address ~~of a terminal~~ that serves as the address of ~~a~~ the terminal 124$_i$ that is to ~~which~~ receive the data ~~arranged~~ stored in the payload of a section ~~is distributed~~. When it is necessary to encrypt the data ~~arranged~~ located in the payload ~~of a section, namely an IC~~, such as for an IP packet ~~here~~, the transmission processing device 113 retrieves an encryption key assigned to the MAC address of ~~a terminal 124i as an address to be arranged in the header of a section~~ the terminal 124$_i$ for arrangement within the section header. The encryption key is retrieved from the encryption key table stored in the encryption key table storage unit 113A~~, with the use of which~~ and is used to encrypt an IP packet arranged in the payload of that section ~~is to be encrypted~~.

[0109]The encryption key table may be of the same type ~~of~~ as a key table ~~that~~ of a receiving apparatus 122 ~~(to be described later) has,~~ or may be of a different type. ~~In this instance, an~~ The encryption key table ~~is~~ may be incorporated into a transmission system 101~~, however, it~~ or may be stored in a server (not shown ~~in figure)~~) in a network 104~~, which may be~~ and retrieved ~~for use~~ through ~~the~~ a circuit connection device 115 ~~as occasion arises~~.

[0110]~~Comprising a modem, TA (Terminal Adaptor), and DSU (Digital Service Unit), etc. for example, the~~The circuit connection device 115 comprises a modem, a Terminal Adaptor (TA), a Digital Service Unit (DSU), etc. for example. The circuit connection device 115 ~~performs~~ carries out communication control over the network 104.

[0111]A reception system 103 ~~consists of~~ includes an antenna 121, the receiving apparatus 122, the circuit connection device 123, the ~~terminal~~ terminals 124_1, 124_2,··· , and the cable 125~~, and the~~. The antenna 121, the receiving apparatus 122, the circuit connection device 123, and the ~~terminal~~ terminals 124_1, 124_2, ··· are connected to each other ~~with~~ via the cable 125 to form a LAN such as ~~the~~ an Ethernet~~(trademark),~~,™ for example.

[0112]The receiving apparatus 122 and the ~~terminal~~ terminals 124_1, 124_2,··· ~~are~~ may be computers, for example. Though ~~In this instance,~~ the receiving apparatus 122 and the ~~terminal~~ terminals 124_1, 124_2,···are shown connected to each other with the cable 125 to form a LAN, ~~but~~ they may instead be connected directly. Furthermore, the receiving apparatus 122 may be a board that can be inserted into a slot of a computer such as a terminal 124_i. Also, the receiving apparatus 122 and circuit connection device 123 may be constituted in a singular computer.

[0113]Satellite ~~broadcasting~~ broadcast waves transmitted from the transmission system 101 via the satellite 102 are received by the antenna 121~~, which~~ and are fed to the receiving apparatus 122. The receiving apparatus 122 ~~applies a process to be described later to~~ processes the received signals, and the resultant data ~~of which~~ is supplied to a specific terminal 124_i.

[0114]~~Formed similarly~~Similar to the circuit connection device 115, the circuit connection device 123 ~~is designed to perform~~ performs communication control over the network 104.

[0115]Each terminal 124_1, 124_2, ··· ~~is~~ may be a computer, for example, ~~and~~ which receives necessary data from the receiving apparatus 122, and conducts ~~such~~ processes such as displaying, outputting, and storing ~~it.~~ the data.

[0116]~~Next, explanation is given on a~~A data transmission process performed by the transmission system 101~~, referring~~ is described with reference to a flowchart shown in Fig. 8.

[0117]First, as shown at ~~the~~ step SP101, the control device 111 judges whether ~~there exists data to be transmitted~~ data is present for transmission to a terminal 124_i. The control device 111 uses ~~Having~~ a schedule table ~~with~~ comprising a schedule to be transmitted ~~described on it, the control device 111 judges based on that schedule table whether there exists data to be transmitted to the terminal 124i. The terminal 124i is designed to be capable of demanding~~ to judge whether such data exists. The terminal 124_i may demand data from the transmission system 101 over the network 104 by controlling the circuit connection device 123, and the control device 111 ~~judges whether there exists data to be transmitted to the terminal 124i,~~ may judge whether such data exists depending upon whether ~~such a demand is received by~~ the circuit connection device 115 receives such a demand over the network 104.

[0118]When ~~it is judged at the step SP101 that there exists no data to be transmitted~~data for transmission to the terminal

124_1 exists, the control device 111 proceeds to the step SP102 and judges whether to change a period. The ~~In the~~ transmission system 101 ~~it~~ is designed ~~such that~~ with encryption keys ~~described on the~~ that are held in an encryption key table in the encryption key table storage unit 113 and that are renewed periodically or in irregular ~~periods, where a~~ intervals. A period in which ~~encryption is performed~~ data is encrypted using an encryption key obtained as a result of a renewal every other time starting from a second time, for example, is called an Even period~~, and where a~~. A period in which ~~encryption is performed with the use of~~ data is encrypted using an encryption device obtained as a result of a renewal every other time starting from a first period is called an Odd period. ~~Accordingly, with Even periods and Odd periods alternating, it is judged at the step SP2~~ The control device 102 judges at the step SP 102 whether it is the time to change from an Even period to an Odd period~~,~~ or to change from an Odd period to an Even period.

[0119]When ~~it is judged~~the control device 111 judges that a period is not to be changed, namely, that it is~~, continuing~~ to continue to encrypt data ~~with~~ using the ~~use of an~~ encryption key presently being used ~~presently in encrypting~~, it returns to the step SP101~~, resulting in repetition of the foregoing processes.When it is judged~~ to repeat the process. When the control device judges that a period is to be changed ~~at the step SP102, that is, changing~~ from an Even period to an Odd period~~,~~ or from an Odd period to an Even period, it proceeds to the step SP103~~,~~ where the control device 111 replaces an encryption key stored ~~on~~ in the encryption key table with an encryption key previously created at the step SP104 ~~to be described later. In this way encryption is performed thereafter with the use of the renewed encryption key~~. Encryption at the transmission processing device 113 is thereafter performed using the encryption key ~~.~~

[0120]At the step SP104, the control device 111 creates ~~(or obtain)~~ or obtains an encryption key that is to be used for the next period~~, which is supplied~~ and supplies the key to the transmission processing device 113~~,~~ which transmits it as the decoding key. Then, ~~it~~ the control device 111 returns to the step ~~SP101, where processes similar to those in the foregoing case are repeated. For additional information, the transmission of a~~ shown at SP101. The transmission of the decoding key may be carried out over a network as well as via the satellite 102.

[0121]~~That is, when~~When a new decoding key ~~used~~ for use in the next period is transmitted to a reception system 103 ~~just~~ before the start of the next period, it ~~may happen~~ is possible that the ~~setting of a~~ new decoding key may not be sent in time for the start of the next period. ~~To cope with it, in this embodiment a~~ Therefore, the new encryption key used in the next period is ~~arranged to be~~ distributed to the reception system 103 ~~in just the~~ during a previous period.

[0122]On the other hand, when ~~it is judged that there exists data~~ the control device judges that data exists to be transmitted to a terminal 124_i, the control device 111 lets the transmission processing device 113 transmit the data ~~to be~~

~~transmitted~~ by controlling the data server 112 or the circuit connection device 115. Upon the receipt of the data ~~supplied~~ from the data server 112 or from the circuit connection device 115, the transmission processing device 113 packets ~~it~~ the data into IP packets~~,~~ and ~~it~~ proceeds to the step shown at SP105.

[0123]The transmission processing device 113 judges, as shown at the step SP105, whether it is necessary to encrypt the IP packet, and when it is ~~judged as one~~ not necessary ~~to be encrypted, it~~, the device 113 proceeds directly to the step SP108~~, skipping the steps SP106 and SP107~~.

[0124]~~Whereas, when~~When the IP packet is judged ~~at the step SP105~~ as one ~~needed~~ that is to be encrypted, ~~it~~ the device 113 moves on the step SP106~~, then the information processing device 113~~ and retrieves an encryption key assigned to the MAC address of a terminal 124$_i$ ~~to be the address of that IP packet~~ from the encryption key table~~, and goes on to the~~. Then, step SP107~~. At the step SP107~~, the transmission processing device 113 encrypts the IP packet ~~with~~ using the ~~key~~ retrieved ~~at the step SP106,~~ key and proceeds to the step SP108.

[0125]~~At the~~As step SP108 shows, the transmission processing device ~~operates~~ uses a ~~CRC (~~Cyclic Redundancy Checking ~~) code (or, check sum) with regard to~~ code (CRC) or checksum on the IP packet. As a result, a section as shown in Fig. 9~~(A)~~(A) is formed ~~with that~~ having the IP packet as the payload ~~appended with a~~, the CRC code at ~~the~~ its bottom, and ~~a~~ the section header at ~~the~~ its top. A stuffing byte is inserted between the payload and CRC, if needed.

[0126]The section header is composed of 3 bytes (96 bits), as shown in Fig. 9~~(B)~~(B). Detailed explanation of the section header is ~~omitted here as it is~~ described in the foregoing EN 301 192 V1.1.1(1997-12) standard, but it should be noted that a ~~MAC address of 48 bits to become an address is arranged between the MAC address 1 and~~ 48-bit MAC address is divided among the MAC addresses 1 to 6. Arranged at the MAC address 1 are ~~8 bits~~ eight of the highest bits of the MAC address, and arranged at the MAC address 2 are the next highest ~~8~~ eight bits. Similarly, ~~8~~ successive eight bits of the MAC address are arranged at each of the MAC addresses 3 to 5, respectively, ~~and~~ with the lowest 8 bits of the MAC address located at the MAC address 6.

[0127]After constituting a data section, the transmission processing device 113 divides that section into payloads each having a given length~~, and performs encapsulation to form a packet of the TS packet type by appending to each payload~~. The processing device then encapsulates the payload to form a TS type packet by appending the header of the TS packet ~~forming a~~ to each payload to form a MPEG 2 transport stream ~~of MPEG 2~~. Then, the transmission processing device 113 proceeds to the step SP109, where ~~such necessary processes as~~ modulation ~~and~~, amplification, etc. are ~~applied to~~ carried out on the resultant packet~~, (which~~. The packet is called a TS packet hereinafter~~, for this~~ because the packet can be ~~basically~~ processed in a similar way as for the TS packet~~), which~~. The TS packet is transmitted as satellite broadcasting waves from the antenna 114, and then ~~it~~ the device 113 returns to the step SP101.

[0128]~~In~~As shown in the section header ~~shown in Fig. 9 (B), the PSC (payload_scrambling_control) of 2 bits~~ in Fig. 9(B), a payload scrambling control (PSC) of 2 bits length is located at the 43rd bit and 44th ~~bit from the first is to be~~ bits. One bit is used, for example, as ~~the~~ an encryption judgment flag to indicate whether data arranged in the payload of the section ~~has been~~ is encrypted, and the other bit is used as a period judgment flag ~~to denote which period, Even or Odd, the data is in.~~ that denotes whether the data is in and Even or Odd period.

[0129]~~To be concrete, for example~~Specifically, the lower bit of the PSC is ~~used as~~ the encryption judgment flag~~, being~~ and has the value 1 when the data has been encrypted~~,~~ and has the value 0 when the data is not encrypted. The higher bit of the PSC is used as the period judgment flag~~, being~~ and is of value 0 in an Even period~~,~~ and of value 1 in an Odd period. ~~However, it is possible to use~~ Alternatively, the higher bit of the PSC may be used as the encryption judgment flag, and the lower bit may be used as the period judgment flag. It is also possible to ~~make~~ assign the ~~assignment~~ values of 0 and 1 ~~as~~ to the encryption judgment flag and ~~the assignment of 0 and 1 as~~ to the period judgment flag ~~by~~ to have the ~~reverse method~~ opposite meanings of the above ~~case~~.

[0130]In the EN 301 192 V1.1.1(1997-12) ~~it is stipulated that~~ standard, when the PSC is of value 00B~~(~~, where B indicates that the value ~~arranged~~ shown before it is a binary number~~)~~, data has not been encrypted. Accordingly, it is preferable to

~~make~~ define the encryption judgment flag to be of value 1 when data has been encrypted~~,~~ and of value 0 when not encrypted, resulting in ~~the~~ conformity ~~to~~ with the DVB specification ~~of the DVB~~.

[0131]As described ~~hitherto~~ above, in the broadcasting system shown in Fig. 7, ~~since~~ data is encrypted ~~with the use of~~ using an encryption key assigned to the MAC address ~~inherent~~ corresponding to each terminal 124_i. Thus, each terminal 124_i can be controlled with regard to reception, ~~thus~~ thereby realizing ~~the~~ an ultimate conditional access mechanism.

[0132]~~As to the method to realize~~The Japan Patent Laid Open No. 215244/1998, by the applicant of the present invention, discloses in detail the method of realizing a conditional access mechanism for performing exact reception control by assigning an encryption key to the value inherent to the receiving side, such as a MAC address or an IP address, ~~details are disclosed in the Japan Patent Laid Open No. 215244/1998 applied by the applicant of this invention. However, with~~. However, the communications satellite broadcasting of Japan ~~conforming~~ conforms to a specification derived from the ~~DVB-SI (~~Digital Video Broadcasting - Service Information / EN300 468 ~~),~~(DVB-SI), and the use of the MAC address ~~is to conform~~ conforms to that specification.

[0133]Next, ~~the~~ Fig. 10 shows ~~a structural~~ an example of ~~a~~ the structure of the receiving apparatus 122 shown in Fig. 7.

[0134]The antenna 121 receives satellite broadcasting waves transmitted from the transmission system 101 via the satellite 102, and the received signals are ~~output~~ outputted to a front-end unit 131. The front-end unit 131 selects the signal of a specific channel from ~~among~~ the signals ~~coming through~~ received by the antenna 121 under the control of a CPU 134, ~~which~~ and the signal is further decoded to a digital stream~~(IP_datagram_data_byte)~~, such as an IP datagram data byte of a TS packet, and ~~is output~~ delivered to a demultiplexer 132. The demultiplexer 132 extracts a specific TS packet ~~out of~~ from the digital stream coming from the front-end unit 131, also under the control of the CPU 134, and ~~is output~~ sends the TS packet to a decoding ~~LSI (~~Large Scale Integrated ~~Circuit) 133. That is to say, the demultiplxer 132 makes a selection of TS packets on the basis of a PID (Packet Identification)~~(CSI) Circuit 133. That is, the demultiplexer 132 selects TS packets based on the Packet Identification (PID) arranged in the header of ~~a TS packet forming a digital stream, coming from the front-end unit 131, and outputs the only selected TS packet~~ the TS packet, and outputs only the selected TS packets to the decoding LSI device 133.

[0135]The decoding LSI device 133 is a one-chip LSI ~~consisting of~~ device comprising a filter 141, a decoder 142, a key table storage unit 143, a checker 144, and a ~~FIFO (~~First In First Out (FIFO) buffer 145.

[0136]The filter 141 examines the data, ~~if~~ when needed, that is arranged in the payload of a section ~~composed~~ comprised of TS packets ~~coming~~ received from the demultiplexer ~~133,~~ 132, destroys ~~the~~ unneeded TS packets, and ~~outputs the~~ delivers only the needed TS packet to the decoder 142.

[0137]The decoder 142 decodes ~~data (here, IP packets)~~ the IP packets arranged in the payload of ~~a section consisting of~~ the TS packets ~~coming~~ that come from the filter 141 ~~with the use of~~ using a decoding key stored in the key table storage unit 143, and outputs the resultant to the checker 144. Also, as explained ~~in~~ regarding Fig. 8, ~~with~~ an encryption key is renewed in the transmission system 101, and when the renewed encryption key is transmitted, the decoder 142 renews the content ~~stored in~~ of the key table storage unit 143 ~~with~~ using that encryption key as the decoding key and under the control of CPU 134. Accordingly, the common key cryptosystem is used as the encryption method ~~in this instance~~. However, the public key cryptosystem~~, too,~~ may also be used as an encryption method.

[0138]The key table storage unit 143 stores a key table ~~onto~~ in which the MAC addresses corresponding to the terminals 124_1, 124_2,~~ ···, which are connected to each other with the cable 125, and~~..., and in which decoding keys assigned to the MAC addresses are registered in correspondence with each other.

[0139]The checker 144 performs error detection on the IP packets ~~output~~ outputted by the decoder 142~~, with the use of~~ using the CRC code of a section ~~arranged~~ located in that IP packet, under the control of CPU 134, ~~thus judging~~ to judge whether decoding is performed correctly in the decoder. The IP packets processed ~~in~~ by the checker 144 are fed to the FIFO buffer 145~~, which~~ that temporarily retains the IP packets ~~coming from the checker 144,~~ and outputs ~~it~~ them to the ~~I/F (Interface)~~ Interface (I/F) 135 under the control of CPU 134.

This process results in adjusting the data rate of the IP packets.

[0140]The CPU 134 controls the front-end unit 131, the demultiplexer 133, the decoding LSI 133, and the I/F 135. The I/F 135 functions as ~~the~~ an interface ~~to supply~~ that supplies the IP packets from the FIFO buffer 145~~,~~ to a terminal 124_i through the cable 125 under the control of CPU 134.

[0141]~~Next, the~~Fig. 11 shows ~~a structural~~ an example of the structure of the key table stored in the key table storage unit 143 in Fig. 10.

[0142]The key table ~~is made up of~~ contains the same number of entries as that of terminals 124_1, 124_2 … ~~connected to the cable 125 for example. In Fig. 11 the~~. The key table contains N ~~pieces~~ units of entries #1 to #N~~, therefore, in the present embodiment,~~ so that the cable 125 is connected to the N number of terminals 124_1 to 124_N. The maximum number of entries on the key table is restricted by the storage capacity, etc. of the key table storage unit 143.

[0143]Registered on each entry #i~~(I~~, where i=1,2,..., N~~)~~, are the MAC address ~~MACaddress~~#i of 48 bits of a terminal 124~~i~~$_i$ and a decoding key of m bits~~(~~, where m denotes a cryptosystem in use~~)~~, assigned to that MAC address~~, in correspondence with each other~~. As explained above, ~~in the present mode of embodiment there exist~~ an Even period and an Odd period ~~with encryption performed~~ exist with a different encryption key ~~in~~ with each period so that two decoding keys are registered in each entry #i~~; a~~. A decoding key ~~(called~~ called an "Even decoding key" ~~hereinafter)~~, hereinafter referred to as $K_{Even\#i}$, is issued to decode data encrypted in an Even period, and ~~a decoding key (called~~ an "Odd decoding key" ~~hereinafter)~~, hereinafter $K_{Odd\#i}$, is issued to decode data encrypted in an Odd period.

[0144]Furthermore, a Valid bit, ~~(~~called an "entry Valid bit" hereinafter~~) indicating~~, indicates whether ~~that~~ the entry #i is valid and is appended to the head of the MAC address ~~MACaddress~~#i of each entry #i. Also, a Valid bit~~(called~~, called a "decoding key Valid bit" hereinafter~~) indicating~~, that indicates the validity is appended to each of Even decoding key $K_{Even\#i}$ and Odd decoding key $K_{Odd\#i}$.

[0145]As to the entry Valid bit and decoding key Valid bit, the value "1" denotes valid, and the value "0" denotes invalid for example. However, it is also possible to ~~apply a method reverse~~ have the opposite value to the above case ~~to the assignment~~ when assigning the value of the entry Valid ~~bit~~ and decoding key Valid ~~bit~~ bits, "0" and "1".

[0146]As described before, in the transmission system 101, a decoding key ~~equivalent~~ that corresponds to a new encryption key ~~used in~~ for the next period is ~~to be~~ distributed to the reception system 103 just ~~bnefore~~ before the next period. Accordingly, ~~a~~ an Odd decoding key ~~(Odd decoding key) equivalent~~ that corresponds to an encryption key ~~to be used in~~ for the next Odd period is distributed in an Even period, and ~~a~~ an Even decoding key ~~(Even decoding key) equivalent~~ that corresponds to an encryption key ~~to be used in~~ for the next Even period is distributed ~~in~~ during an ~~ODD~~ Odd period. ~~And, in~~ In the decoder 142, decoding keys that are distributed in such a manner are ~~set up (overwrite, for example) on~~ retained by an overwrite, for example, within the key table. Therefore, ~~in this case,~~ a decoding key that is to be used in the next period is set up ~~on~~ in the key table ~~until~~ before the current period terminates. Furthermore, ~~since~~ because the ~~changing~~ change of decoding keys ~~accompanying with~~ that accompanies the ~~changing~~ change of periods ~~can~~ may be performed simply by switching the position~~(address)~~, i.e., the address of the key table from which the decoder 142 ~~performs retrieving~~ retrieves, without involving CPU34, ~~it~~ the change can be done ~~in a moment.~~ rapidly.

[0147]~~Next, explanation will be given on the~~The operation of a receiving apparatus in Fig. 10 is now explained with reference to a flowchart shown in Fig. 12.

[0148]The antenna 121 receives satellite ~~broadcasting~~ broadcast waves transmitted from the transmission system 101 via the satellite 102, ~~and~~ the received signals ~~obtained~~ are transformed into ~~the~~ a digital stream of a TS ~~packet through the~~ packets via front-end unit 131 and the demultiplexer 133, and ~~are~~ the signal stream is supplied to the decoding LSI 133.

[0149]In the decoding LSI 133, a section ~~consisting~~ of TS packets output by the demultiplexer 132 is supplied to the decoder 142 ~~through~~ via the filter 141. Upon the receipt of the section, the decoder 142 ~~sets~~ retains the MAC address arranged in the section header ~~to~~ as a variable MA ~~as~~ in a built-in register.

[0150]The decoder 142 retrieves the stored entry of ~~a~~ the MAC address ~~coinciding~~ that coincides with the variable MA by referring to the key table, ~~that is to say, reads~~ as step SP 111 shows. The decoder reads, in order, a MAC address registered in each entry #i starting from the entry #1 of the key table ~~in order~~, and compares ~~(checking)~~ by checking the MAC address read and the variable MA to ~~judge~~ determine whether ~~there exists the entry of~~ a MAC address ~~matching~~ entry matches the variable MA, as shown at the step SP112. When ~~it is judged at the step SP112 that there exists no entry of a MAC address matching~~ there is no MAC address entry that compares to the variable MA, namely~~,~~ when ~~a~~ no terminal having ~~a~~ the MAC address arranged in the section header is ~~not~~ connected to the cable 125, the decoder 142 proceeds to the step shown at SP113, and destroys the section supplied, thereby terminating the processing.

[0151]Also, when ~~it is judged at the step SP112 that there exists the~~ there is an entry of a MAC address ~~matching~~ that compares to the variable MA, ~~it~~ the decoder 142 proceeds to the step shown at SP114 with ~~that~~ the entry ~~regarded~~ it regards as the marked entry.

[0152]The decoder 142 judges, at the step SP114, whether that marked entry is valid~~,~~ based on the ~~entry~~ Valid bit of the marked entry. When ~~it is judged at the step SP114 that~~ the marked entry is not valid, namely when the ~~entry~~ Valid bit is "0", the decoder 142 proceeds to the step shown at SP113, and destroys the section supplied, thus terminating the processing. Thus ~~Accordingly~~, even when a terminal ~~having a~~ exists that has the MAC address arranged in the section header of a section supplied to the decoder 142 ~~is connected to the~~

~~cable 125~~, if the entry of that MAC address is not valid, the section is not supplied to ~~the~~ that terminal ~~connected to the cable 125~~.

[0153]When the marked entry is ~~judged to be valid at the step SP114~~ valid, that is~~,~~ when the ~~entry~~ Valid bit of the marked entry is "1", ~~it~~ the decoder 142 proceeds to the step SP115~~,~~ and ~~the decoder 142~~ judges whether the data ~~(IP packet)~~ i.e., the IP packet in the payload of the section, has been encrypted~~, with reference to~~. The decoder 142 judges using the lower bit of the PSC ~~(Fig. 9 (B))~~ of the section header shown in Fig. 9(B), namely the encryption judgment flag. When the encryption judgment flag is ~~judged~~ determined to be "0" ~~at the step SP115~~, that is~~,~~ when the IP packet arranged in the payload of the section has not been encrypted, the decoder 142 proceeds ~~to the step SP119, skipping the steps SP117 and SP118, and outputs that~~ directly to the step shown at SP119, and outputs the unencrypted IP packet to the FIFO buffer 145 ~~through~~ via the checker 144, thereby terminating ~~the~~ processing. The ~~And, the~~ IP packet stored in the FIFO buffer 145 is then supplied to a terminal 124$_i$ ~~connected to the cable 125 through the I/F 135, which is~~ specified by the MAC address in the section header of the section arranged in that IP packet.

[0154]~~Whereas,~~When the decoder judges that the encryption judgment flag is ~~judged to be "1"~~ of value "1", as shown at the step SP115, that is~~,~~ when the IP packet arranged in the payload of the section is encrypted, ~~it~~ the decoder goes on to the step SP116~~,~~ and ~~the decoder 142~~ sets the higher bit of the

PSC ~~(Fig. 9 (B))~~ of the section header of that section, namely the period judgment flag~~, to~~ shown in Fig. 9(B), to the value of the variable EO ~~as being~~ in a built-in register, and then proceeds to the step SP117.

[0155]The decoder 142 judges, as shown at the step SP117, whether the decoding key Valid bit # (MA, EO) is valid ~~in~~ during a period corresponding to the variable EO in the marked entry in which the MAC address matches the variable MA~~, that is, in~~. That is, the decoder 142 judges during an Even period when the variable EO is “0”~~,~~ and ~~in~~ during an Odd period when the variable EO is “1”. When ~~it is judged that~~ the decoding key Valid bit # (MA, EO) is not valid, that is~~,~~ that the decoding key Valid bit # (MA, EO) is “0”, ~~it~~ the decoder proceeds to the step SP113~~,~~ and ~~the decoder 142~~ destroys the section supplied, thus terminating ~~the~~ processing. Accordingly, even when a terminal exists having ~~a~~ the MAC address arranged in the section header of the section supplied to the decoder 142 ~~is connected to the cable 125~~ and the entry of that MAC address is valid, if the decoding key ~~in~~ during a period indicated by the period judging flag is not valid, that section is not supplied to the terminal ~~connected to the cable 125~~.

[0156]On the other hand, when the decoding key Valid flag # (MA, EO) is judged to be valid ~~at the step SP117~~, namely when the decoding key Valid flag # (MA, EO) is “0”, ~~it~~ the decoder proceeds to the step SP118~~, and the decoder 142 retrieves the decoding key (MA, EO) in a period matching the variable EO in the marked entry where the MAC address coincides with the~~

~~variable MA~~ and retrieves, from the key table, ~~and~~ the decoding key (MA, EO) during a period matching the variable EO in the marked entry where the MAC address coincides with the variable MA. The decoder decodes the IP packet arranged in the payload of the section using the decoding key (MA. EO)~~,~~ and then ~~it~~ proceeds to the step SP119.

[0157]The decoder 142 outputs the decoded IP packet to the FIFO buffer 145 ~~through~~ via the checker 144 ~~at the~~, as step SP119 shows, and ~~the~~ processing is terminated. Also ~~And~~, the IP packet stored in the FIFO buffer 145 is supplied to a terminal 124$_i$ ~~connected to the cable 125,~~ specified by the MAC address in the section header of the section having the IP packet ~~through the I/F 135~~.

[0158]~~Processes following~~The process of the flowchart in Fig. 12 is performed every time a section is supplied to the decoder 142. As described ~~hitherto~~ above, the validity of the entry is judged based on the entry Valid bit ~~registered~~ stored in the entry of the key table, and the output of data to a terminal is controlled, so that it is possible to easily ~~restricts~~ restrict users ~~(terminals)~~ or terminals to obtain ~~(receive)~~ or receive data correctly. Furthermore, ~~since~~ because the data output ~~of data~~ is controlled ~~based on~~ by the value of the decoding key Valid bit of the key table, ~~it can be easily practiced to allow a certain terminal~~ a respective terminal may easily be allowed to receive data in ~~the~~ only one period, either ~~in~~ during an Even period or Odd period, or ~~to prohibit it~~ may be prohibited from receiving data in either ~~one~~ period. The setting of values of the entry Valid bit and the decoding key Valid bit can be done in a receiving apparatus 122 independently, or may be done based on the information transmitted from the transmission system 101.

[0159]In this embodiment, a decoding key~~(~~, as well as an encryption key~~)~~, is assigned to the MAC address inherent to a terminal~~, however~~. However, it is also possible to ~~decide~~ define a terminal ~~ID (Identification)~~ Identification (ID) inherent to a terminal~~,~~ and ~~to~~ then assign a decoding key to that terminal ID. Furthermore, ~~it is also possible to determine~~ a group ID inherent to a plurality of terminals may be designated, and ~~to assign~~ a decoding key assigned to that group ID. However, when assigning a decoding key to a MAC address, ~~it is possible to easily incorporate~~ an exact conditional access mechanism may easily be incorporated, as described hitherto, into the outline of digital satellite broadcasting based on the EN 301 192 V1.1.1 (1997-12) standard, which is the DVB ~~standards.~~standard.

[0160]In this embodiment, the one-chip decoding LSI 133 comprises the filter 141, the decoder, 142, the key table storage unit 143, the checker 144, and the FIFO buffer 145~~, however~~. However, it is also possible to ~~separately~~ form a filter 141, decoder~~,~~ 142, key table storage unit 143, checker 144, and FIFO buffer 145 as ~~one chip~~ separate chips. However, the employment of a one-chip decoding LSI 133 ~~incorporating a filter 141, decoder, 142, key table storage unit 143, checker 144, and FIFO buffer 145 may increase the~~ increases security because the data decoding ~~of data~~ is performed within the single decoding LSI 133, and is completely ~~sheltered~~ removed from the outside. Furthermore, ~~from the viewpoint of the reducing of~~ to reduce the installation area of circuits and high-speed processing, it is preferable to ~~incorporate the filter 141, the decoder, 142, the key table storage unit 143, the checker 144, and the FIFO buffer 145 into~~ use a one-chip decoding LSI 133.

[0161] Further, in this embodiment, ~~explanation is given on the case where data is distributed by~~ the digital satellite broadcast~~, however~~ distributes the data. However, the present invention may be applied to ~~such~~ a case where the data is distributed ~~by the~~ using a multicast, for example.

[0162] Further, in the present embodiment, two types of periods, namely Even ~~period~~ and Odd ~~period,~~ periods, are provided~~, however~~. However, it is also possible to not ~~to~~ use such periods, or to provide more than two types of periods. Likewise, it is possible to have ~~the~~ only one decoding key or more than two decoding keys ~~registered into~~ associated with each entry of the key table.

[0163] In the present embodiment, data is distributed ~~in a form~~ based on the DVB standards~~, however,~~. However, data may instead be distributed in a form, not based on the DVB standards. Moreover, ~~Next, a series of~~ the foregoing processes ~~can~~ may be performed not only with hardware but also with software. ~~In the case of performing the series of processes with software~~ Namely, a program constituting the software is installed on a general-purpose computer or one-chip microcomputer.

[0164] Fig. 13 shows ~~a structural example of one embodiment of~~

~~a computer installed~~ an example of the structure of a further embodiment in which a computer is provided with a program performing ~~a series of~~ the foregoing processes.

[0165]A program ~~may be~~ is stored in ~~advance into~~ a storage medium, such as a hard disk 205 or ROM 203, which is built into a computer.

[0166]~~Or~~Alternatively, a program may be stored ~~(recorded)~~ or recorded, either temporarily or perpetually, in a removable recording medium 211 such as a floppy disk, ~~CD-ROM (~~Compact Disc Read Only Memory ~~), MO (Magneto Optical) disc, DVD (~~(CD-ROM), Magneto Optical (MO) disc, Digital Versatile Disc ~~)~~(DVD), magnetic disc, or semi-conductor memory. ~~Such~~ A removable recording medium 211 may be provided as ~~the so-called package software.~~ a software package.

[0167]~~Not only installed into a computer from the foregoing~~Instead of a removable recording medium 211, ~~but~~ a program may be transferred ~~by wireless from a download site to a computer~~ to a computer using a wireless connection, such as from a download site via an artificial satellite link for digital satellite broadcasting, or may be transferred ~~to a computer by wire~~ using a wire connection over a network, such as ~~LAN (~~a Local Area Network ~~)~~(LAN) or the Internet. The computer receives such ~~programs~~ transferred programs at ~~the~~ a communications unit 208~~,~~ which can be installed in the built-in hard disk 205.

[0168]The computer incorporates a ~~CPU (~~Central Processing Unit ~~) 202. Connected~~(CPU) 202 that is connected to an input/output interface 210 ~~with~~ via a bus 201~~, the~~. The CPU 202 executes a program stored in a ~~ROM (~~Read Only Memory ~~)~~(ROM) 203 according to commands ~~which are~~ entered by a user through the input/output interface 210 ~~with~~ using an input unit 207 such as a keyboard and mouse, etc. Also, the CPU 202 loads into a ~~RAM (~~Random Access Memory ~~)~~(RAM) 204 and ~~performs~~ executes programs stored in the hard disk 110, ~~programs~~ which are transferred from a satellite or over a network to the communications unit 208~~,~~ and installed in the hard disk 205, or ~~programs~~ which are installed in the hard disk 205 after being retrieved from the removable recording media 211 ~~installed~~ that is inserted into the drive 209. In this manner, the CPU 202 performs processes ~~following~~ according to the foregoing flowchart~~,~~ or performs processes ~~following~~ according to the structure of the foregoing block diagrams. ~~And~~ Also, the CPU 202 ~~outputs~~ may output, when required, the processed results ~~from the~~ to an output unit 206, such as ~~an LCD (~~a Liquid Crystal Display ~~)~~(LCD) or a speaker, etc., through ~~the~~ an input/output interface 210, or ~~transmits them~~ the CPU may transmit the output from the communications unit 208~~, and furthermore, lets~~. Furthermore, the CPU may transmit the output to the hard disk to record ~~them.~~the output.

[0169]As to the present specification, the above processing steps ~~describing~~, which describe a program to ~~let~~ permit the computer perform various processes, are not necessarily followed in a time ~~series~~ sequence along the order described ~~as~~ in the flowchart~~, but~~. Rather, the specification includes processes ~~to~~ that may be performed concurrently or individually~~(e.g.,~~, e.g., using concurrent processing or processing with objects~~)~~.

[0170]Also, the programs may be those ~~which~~ that are processed by a single computer~~,~~ or by a plurality of computers ~~in~~ using distributed processing. Furthermore, the programs may be ~~those which are~~ transferred to a computer located in a faraway site for execution. ~~to be performed.Industrial Applicability~~ The present invention can be utilized for the data transmission system using the digital satellite broadcasting and the data transmission system using the wired network.

~~Explanation of Reference Numerals~~

~~1 satellite data transmission system 2 transmission system, 3 satellite, 4 reception system, 5 Internet, 10 control device, 11 circuit connection device, 12 data server, 13 transmission processing device, 14 local network, 15 transmitting antenna, 20 receiving antenna, 21 receiving apparatus, 22 information processing device, 23 circuit connection device, 24 local network, 30 CPU, 31 front end unit, 32 demultiplexer, 33 receiving filter, 34 decoding unit, 35 checker, 36 buffer, 37 key table, 38 interface unit, 39 bus, 101 --- transmitting system, 102 --- satellite, 103 --- receiving system, 104 --- network, 111 --- control device, 112 --- data server, 113 --- transmission processing device, 113A --- encryption key table storage unit, 114 antenna, 115 --- circuit connection device, 116 --- cable, 121 --- antenna, 122 --- receiving apparatus, 123 --- circuit connection device, 1241', 1242 --- terminal, 131 --- front-end unit, 132 --- demultiplexer, 133 --- decoding LSI, 134 --- CPU, 135 --- I/F, 141 --- filter, 142 --- decoder, 143 --- key table storage unit, 144 --- checker, 145 --- FIFO buffer, 201 --- bus, 202 --- CPU, 203 --- ROM, 204 --- RAM, 205 --- hard disk, 206 --- output unit, 207 --- input unit, 208 --- communication unit, 209 drive, 210 --- input/output interface, 211 --- removable storage medium.~~

~~14/14~~